ESC-TR-97-143

Quarterly Technical Summary

Advanced Electronics Technology

15 August 1998

Lincoln Laboratory
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LEXINGTON, MASSACHUSETTS

Prepared for the Department of the Air Force under Contract F19628-95-C-0002.

This report is based on studies performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. The work was sponsored by the Department of the Air Force under Contract F19628-95-C-0002.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

Gary Tutungian
Administrative Contracting Officer
Contracted Support Management

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

ADVANCED ELECTRONICS TECHNOLOGY

QUARTERLY TECHNICAL SUMMARY REPORT
TO THE
AIR FORCE MATERIEL COMMAND

1 MAY – 31 JULY 1998

ISSUED 17 NOVEMBER 1998

Approved for public release; distribution is unlimited.

LEXINGTON MASSACHUSETTS

INTRODUCTION

This Quarterly Technical Summary covers the period 1 May through 31 July 1998. It consolidates the reports of Division 6 (Communications and Information Technology) and Division 8 (Solid State) on the Advanced Electronics Technology Program.

TABLE OF CONTENTS

COMMUNICATIONS AND INFORMATION TECHNOLOGY — DIVISION 6

SOLID STATE — DIVISION 8

COMMUNICATIONS AND INFORMATION TECHNOLOGY
DIVISION 6

INTRODUCTION

This section of the report reviews progress on Machine Intelligence Technology during the period 1 May through 31 July 1998. Separate reports describing other Information Systems Technology work of Division 6 are issued for the following programs:

Tactical Speech Technology	AFRL/IFEC
Speech and Signal Processing Technology	NSA

V. W. Chan
Head, Division 6

C. W. Niessen
Associate Head

MACHINE INTELLIGENCE TECHNOLOGY
GROUP 62

1. INTRODUCTION

The objective of the Machine Intelligence Program has been the application of MI techniques to problems in the interpretation and utilization of data produced by imaging sensors. Past emphasis has been on algorithms for ISAR (Inverse Synthetic Array Radar) and SAR (Synthetic Array Radar) imaging sensors and on processors for real-time, fully-automated applications such as automatic recognition of re-entry vehicles (the ISAR application) and of ground vehicles (the SAR application). The image understanding application emphasis has been shifted over the past 18 months to concentrate on exploitation technology for visible and IR multispectral sensors, most particularly night vision research in which low-light visible and IR images are combined to create a color night vision capability. Fusion techniques have also been applied to image enhancement and color display algorithm development to facilitate analyst-based exploitation of multispectral surveillance images, and to multispectral surveillance algorithm research to develop automatic target detection algorithms for operation in complex environments. The line-supported work on night vision was completed last FY, with follow-on work on algorithms, real-time implementation, and low-light CCD sensor technology being funded by DARPA.

Motivated by the growing vulnerability of large-scale military and national information-dependent infrastructure systems to exploitation, manipulation, and sabotage, Lincoln Laboratory conducted a study during FY95 commissioned by DARPA/ITO. The study goal was to recommend technical approaches and technology-based strategies to address this situation, particularly in regard to current and future U.S. Military Communications, Command, Control, Computers, and Intelligence (C4I) systems. Also in the FY95-96 time frame, Lincoln participated in several national studies focused on these issues, including the DARPA Information Science and Technology FY95 summer study on Defensive Information Warfare, and the FY96 Defense Science Board Task Force on Defensive Information Warfare (IW-D). As an outgrowth of these efforts, Lincoln initiated in FY97 an OSD Line-supported IW-D technology development program focused on the following major aspects of this important national security problem:

- Survivable Distributed C4I Systems
- Computer/Network Monitoring and Surveillance

Work in these two areas during the third quarter of FY98 is summarized below.

2. SURVIVABLE DISTRIBUTED C4I SYSTEMS

Work on IW survivable C4I systems has continued to focus on distributed collaborative planning as a prototype application to drive the research.

A system for secure, survivable collaborative planning has been developed by integrating a new, application-level, multicast-capable version of the Internet Security Protocols into a collaborative planning system (from U. C. Berkeley) which includes video, voice, and whiteboard. Lincoln has developed and demonstrated the capability for flexible control of multiple security associations, so that the encryption key as well as the encryption algorithm can be switched on a per-packet basis. This flexibility can be used, for example, to respond rapidly to a situation where one of the members of a small unit operation force is captured, and it is necessary to shut off communication with that member. A connection to an internet-based security association and key management system, which would enable security setup and reconfiguration over an internet, is also planned as part of this system structure, although that connection has not yet been implemented.

Prior work on dynamic protocol reconfiguration could also be integrated with this work on security protocols. Recently, we have developed and demonstrated a prototype conferencing application that uses dynamic reconfiguration as an approach for maintaining operation in the face of potential network attacks against fixed protocols. The dynamic protocol reconfiguration has progressed to a prototype demonstration, but more work is needed to fully develop it and integrate it with an internet conferencing system.

In addition, we have made preliminary measurements on the effectiveness of several denial-of-service attacks against reliable multicast protocols. The test bed we have developed for making these measurements will be useful in evaluating our security protocols and survivability strategies.

3. COMPUTER/NETWORK MONITORING AND SURVEILLANCE

3.1 Overview

During the past quarter, we have used our simulation network to generate six weeks of network traffic and audit log files. These data, containing normal network traffic mixed with attack traffic, are being distributed to more than one dozen DoD contractors who will use the data to evaluate their computer network intrusion detection systems.

Network sessions are generated for a wide variety of services present on a typical Air Force base local area network. These services include, but are not limited to, remote login, remote file transfer, electronic mail, and web traffic. The frequency and character of the network sessions generated for each of these services reflects actual usage of these services at Air Force bases worldwide.

The vast majority of the training data are representatives of normal background traffic. These were generated automatically using special purpose software described in previous quarterly reports. Also included in the six weeks of training data, however, are attack sessions. These attacks can be categorized broadly into three types: unauthorized access, denial of service, and anomalous usage. Many of these attack sessions are run automatically using the same special purpose software used to produce normal traffic, while some of them are run in real-time by human operators typing at a keyboard. Described below is a taxonomy of the attacks found in the training data.

3.1.1 Taxonomy of Attacks

The taxonomy of attacks provides a way of succinctly and definitively classifying attacks. The primary purpose for categorizing attacks here is to create classes from which to draw test case intrusions for evaluating intrusion detection systems (IDSs). Equivalence partitioning categorizes attacks in such a way that an IDS has a roughly equivalent chance of recognizing each member of a class. This simplifies testing by enabling the IDS to be tested against just a few members of each class.

In the following discussion an "intrusion" or "attack" is an instance in which someone gains unauthorized access to a system or disrupts authorized access. "Exploits" are code or methods which take advantage of a vulnerability or security fault to provide unauthorized access. "Vulnerabilities" or "security faults" are flaws in systems that allow attacks to occur. They can be caused by software errors, by providing features that can be misused, or by poor user validation.

3.1.1.1 Privilege Levels

The taxonomy first provides several ways to classify the level of access an attacker has to a system.

O – No Access

R – Remote Network Access

L – Local Network Access

U – User Access

S – Root/Superuser Access

"No Access" means that the user has no practical access to the system, as when the system is in a locked building on a separate network. "Remote Network" access refers to having, via other networks, minimal network access to the system. "Local Network" means having the ability to read and write to the local network that the target system uses. "User Access" refers to having the ability to run normal user commands, and "Root/Superuser Access" gives the user total access to the system.

3.1.1.2 Actions

The taxonomy includes the following five action classes:

1) Probing – Gathering data about a system. More specific categories can be defined such as:
   - Probe (Users) – Users on a machine.
   - Probe (Services) – Services on a machine.
   - Probe (Machines) – Machines on a network.
2) Denial of Service – Hindering legitimate access to the system.
   - Deny (Temporary) – Temporary denial with automatic recovery.
   - Deny (Administrative) – Denial requiring administrator intervention.
   - Deny (Permanent) – Permanent denial of service.
3) Interception / Reading of Files
   - Intercept (Files) – Files on a system.

- Intercept (Network) – Network traffic.

4) Alteration / Creation of Data
   - Alter (Data) – Alter stored data.
   - Alter (Intrusion-Traces) – Remove intrusion traces, such as log files.

5) Attacker Uses System
   - Use (Recreational) – Intruder uses the system for recreational purposes.
   - Use (Productivity) – Using the system for productivity-related purposes.
   - Use (Intrusion-Related) – Using the system resources to help break into other sites.

3.1.1.3 Method of Transition

The user needs to exploit some failure of the security system to perform an attack. Three categories of failure are:

m – Masquerading, i.e., misrepresenting oneself. An example could be using a stolen name/password pair, or sending a TCP packet with a forged source address to a target machine.

a – Abuse of Feature. There are legitimate actions that one can perform that, when taken to the extreme, will lead to system failure. Examples are filling a disk partition with files or a mail spool with junk e-mail, attempting to connect to every port on a system to determine which services are running, or sending huge amounts of network traffic in order to saturate network hardware.

b – Implementation bug. A bug in a trusted program allows an attack to proceed. Specific examples are buffer overflows and race conditions.

3.1.1.4 Examples

SYN Flood: R-a-Deny (Temporary). User needs network access to enact a temporary denial of service.

Sniffing Passwords: L-a-Intercept (Network). User with access to a computer's local network intercepts plain text passwords.

Eject: U-b-S. User exploits bug in eject program to become superuser.

3.1.2 Attacks

We describe below the attacks used in the training portion of the 1998 intrusion detection evaluation corpus.

3.1.2.1 Sources

Most of the attacks used in the development of this evaluation corpus have been drawn from public sources. There are several places on the internet to find information about known computer vulnerabilities. "Bugtraq" is a full-disclosure mailing list on which network administrators and computer security experts announce and discuss computer vulnerabilities. Often, code which exploits these weaknesses will be posted to the list with the stated intent of allowing users to "test" their systems for the vulnerability. The website www.rootshell.com is a repository of known exploits and network attacks, and contains exploit scripts and descriptions of vulnerabilities from any sources. Other attacks were created by using information about potential security holes from security organizations like the CMU CERT (Computer Emergency Response Team). We also created several new attacks. These new attacks are useful for determining how IDSs work against novel attacks—a difficult class of attacks for signature-detection systems to detect.

3.1.2.2 Age of an Attack

Each attack has a period of time during which it is most potent. After a vulnerability is announced, some systems will be patched immediately to protect the system against the vulnerability. As time passes, more and more systems will become resistant to the intrusion as new operating system versions are released and more systems administrators apply the patches. Some systems will go for years without having widely-known security holes fixed. A number of computers in operation today contain these holes, and publicly available scanning programs allow attackers to discover these systems by scanning a large number of hosts (often several Class A subnets) for a vulnerable host. Our set of 20 attacks to be used for the training data contains attacks from all stages of this life cycle. Some are new (announced within the last six months), some are one to two years old, and some have been known for several years. It is expected that many IDSs will find the older attacks quite easily, but may have difficulty with recognizing newer attacks.

3.1.2.3 Stealthiness of Intruders

Stealthiness is defined as taking steps to evade detection by either a human system administrator or an automatic IDS. There are many approaches that an attacker can use to hide from an IDS. For example, many IDSs are keyword-based and may look for a string such as "loadmodule". A hacker could easily fool such an IDS by setting a UNIX shell variable VAR to the string "module" and then issuing the command as "load$VAR". Another way that an IDS can find an intruder is by looking at the output of the command they are issuing. Many systems will give a strong warning if a user prints the contents of the password file (which holds encrypted user passwords) to the screen. A hacker could hide these actions by passing the output of his program through a filter which alters the data before printing it to the screen. The hacker can then apply the inverse filter on the local side of his network connection and the output of his commands will be hidden from a keyword spotting IDS. Another means of hiding from an IDS is to break up the attack into several sessions which occurs over an extended length of time. By separating the exploit (which actually gains access for the attacker) from actions (which will vary greatly depending on the motivation of the attacker), an attacker may be able to break up his attack, which would register a high warning if viewed as a single session, into several rather innocuous looking sessions which would only appear suspicious when considered as a whole.

3.1.2.4 The Twenty Training Data Attacks

Twenty Attack Types to be Used in Training Data
for the DARPA 1998 Off-Line Evaluation

	Solaris	SunOS	Linux
Denial of Service	Ping of Death	Ping of Death	Ping of Death
	neptune	neptune	neptune
	syslogd	teardrop	teardrop
	smurf	smurf	smurf
	back	back	back
Remote to User	dictionary	dictionary	dictionary
	guest	guest	guest
	phf	phf	phf
	ftp-write	ftp-write	ftp-write
			imap
User Root	eject	loadmodule	Perl
	ffbconfig		
	fdformat		
Probing / Surveillance	portsweep	portsweep	portsweep
	ipsweep	ipsweep	ipsweep
	satan	satan	satan

Descriptions

Back: R-b-Deny (Temporary)
If a request to an Apache web server contains a large number n backslashes, the web-server will take O (n^2) time to process the request.

Dictionary: R-a-U
Guess passwords for a valid user using simple variants of the account name over a telnet connection.

Eject: U-b-S
Buffer overflow using eject program on Solaris. Leads to a user to root transition if successful.

Ffbconfig: U-b-S
Buffer overflow using the ffbconfig UNIX system command leads to root shell, if successful.

Fdformat: U-b-S
Buffer overflow using the fdformat UNIX system command leads to root shell, if successful.

Ftp-write: R-a-U

Remote ftp user creates .rhost file in world writable anonymous ftp directory and obtains local login.

Guest: R-a-U

Try to guess password via telnet for a guest account.

Imap: R-b-S

Remote buffer overflow using imap port leads to root shell, if successful.

Ipsweep: R-a-Probe (Machines)

Surveillance sweep performing either a port sweep or ping on multiple host addresses.

Land: R-b-Deny (Administrative)

Denial of service where a remote host is sent a UDP packet with the same source and destination, crashing the remote host if successful.

Loadmodule: U-b-S

Resets IFS for a normal user and creates a root shell, if successful.

Neptune: R-a-Deny (Temporary)

Syn flood denial of service on one or more ports.

Perl: U-b-S

Perl attack which sets the user id to root in a perl script and creates a root shell, if successful.

Phf: R-b-S

Exploitable CGI script which allows a client to execute arbitrary commands on a machine with a misconfigured web server.

Ping of Death: R-b-Deny (Administrative)

Denial of service, where a large ping packet crashes system, if successful.

Portsweep: R-a-Probe (Services)

Surveillance sweep through many ports to determine which services are supported on a single host.

Satan: R-a-Probe (Services)

Network probing tool which looks for well-known weaknesses. Operates at three different levels. Level 0 is light, Level 1 is medium, and Level 2 is heavy.

Smurf: R-a-Deny (Temporary)

Denial of service via flood of ICMP echo replies.

Syslog: R-b-Deny (Administrative)

Denial of service for the syslog service connects to port 514 with unresolvable source IP address.

Teardrop: R-b-Deny (Administrative)

Denial of service where misfragmented UDP packets cause some systems to reboot.

SOLID STATE
DIVISION 8

INTRODUCTION

This section of the report summarizes progress during the period 1 May through 31 July 1998. The Solid State Research Report for the same period describes the work of Division 8 in more detail. Funding is provided by several DoD organizations—including the Air Force, Army, BMDO, DARPA, Navy, NSA, and OSD—and also by the DOE, NASA, and NIST.

D. C. Shaver
Head, Division 8

R. W. Ralston
Associate Head

DIVISION 8 REPORTS ON ADVANCED ELECTRONICS TECHNOLOGY

1 MAY THROUGH 31 JULY 1998

PUBLICATIONS

High-Precision Film Thickness Determination Using a Laser-Based Ultrasonic Technique	M. J. Banet* M. Fuchs* J. A. Rogers* J. H. Reinold, Jr. J. M. Knecht M. Rothschild R. Logan* A. A. Maznev* K. A. Nelson*	*Appl. Phys. Lett.* **73**, 169 (1998)
A 1.3-GHz SOI CMOS Test Chip for Low-Power High-Speed Pulse Processing	R. Berger W. G. Lyons A. M. Soares	*IEEE J. Solid-State Circuits* **33**, 1259 (1998)
Calculated and Measured Transmittance of Metallodielectric Photonic Crystals Incorporating Flat Metal Elements	A. Kao K. A. McIntosh O. B. McMahon R. Atkins S. Verghese	*Appl. Phys. Lett.* **73**, 145 (1998)
Effects of the Internal Loss on Power Efficiency of Mid-Infrared InAs–GaInSb–AlSb Quantum-Well Lasers and Comparison with InAsSb Lasers	H. Q. Le C. H. Lin* S. J. Murray* R. Q. Yang* S. S. Pei*	*IEEE J. Quantum. Electron.* **34**, 1016 (1998)
Damage Testing of Pellicles for 193-nm Lithography	V. Liberman R. R. Kunz M. Rothschild J. H. C. Sedlacek R. S. Uttaro A. Grenville* A. K. Bates* C. Van Peski*	*Proc. SPIE* **3334**, 480 (1998)

*Author not at Lincoln Laboratory.

Assessment of Optical Coatings for 193-nm Lithography	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro A. Grenville* A. K. Bates* C. Van Peski*	*Proc. SPIE* **3334**, 470 (1998)
Thin Silicide Development for Fully-Depleted SOI CMOS Technology	H. I. Liu J. A. Burns C. L. Keast P. W. Wyatt	*IEEE Trans. Electron Devices* **45**, 1099 (1998)
Metrology Methods for the Quantification of Edge-Roughness	C. M. Nelson S. C. Palmateer T. Lyszczarz	*Proc. SPIE* **3332**, 19 (1998)
Line Edge Roughness in Sub-0.18-μm Resist Patterns	S. C. Palmateer S. G. Cann J. E. Curtin S. P. Doran L. M. Eriksen A. R. Forte R. R. Kunz T. M. Lyszczarz M. B. Stern C. Nelson*	*Proc. SPIE* **3333**, 634 (1998)
Screening of Excitons in GaN Crystals	D. C. Reynolds* D. C. Look* B. Jogai* R. J. Molnar	*J. Phys.* **10**, 5577 (1998)
Photolithography at Wavelengths Below 200 nm	M. Rothschild	*Proc. SPIE* **3274**, 222 (1998)
Pattern Transfer for Diffractive and Refractive Microoptics	M. B. Stern	*Microelectron. Eng.* **34**, 299 (1997)

*Author not at Lincoln Laboratory.

Phase Noise of a Resonant-Tunneling Relaxation Oscillator	S. Verghese C. D. Parker E. R. Brown	*Appl. Phys. Lett.* **72**, 2550 (1998)

ACCEPTED FOR PUBLICATION

Bromine Ion-Beam-Assisted Etching of InP and GaAs	W. D. Goodhue D. E. Mull J. M. Rossler Y. Royter C. G. Fonstad*	*J. Vac. Sci. Technol.*
Modeling the Microwave Impedance of High-T_C Long Josephson Junctions	D. E. Oates C. J. Lehner* Y. M. Habib* G. Dresselhaus* M. Dresselhaus*	*J. Superconduct.*

PRESENTATIONS[†]

Photolithography at Wavelengths Below 200 nm	M. Rothschild	1998 Conference on Lasers and Electro-Optics, San Francisco, California, 3-8 May 1998
The Photomixer Transceiver	S. Verghese K. A. McIntosh	
Optical Lithography at Feature Sizes of 0.25 μm and Below	R. R. Kunz	Lincoln Laboratory Technical Seminar Series, University of California, Berkeley, California, 8 May 1998

*Author not at Lincoln Laboratory.

[†] Titles of presentations are listed for information only. No copies are available for distribution.

Microwave Superconducting Devices and Material Nonlinearity	D. E. Oates	Technical Seminar, Texas Center for Superconductivity, University of Houston, Houston, Texas, 8 May 1998
Critical Issues for Projection Lithography at 157 nm	T. M. Bloomstein M. Rothschild M. W. Horn R. B. Goodman D. E. Hardy	42nd International Conference on Electron, Ion and Photon Beam and Nanofabrication, Chicago, Illinois, 26-29 May 1998
Near-Field Optical Lithography at 193 nm	M. W. Horn M. Rothschild R. B. Goodman	
Line Edge Roughness: Measurements, Mechanisms and Impact on Future Lithographies	S. C. Palmateer R. R. Kunz T. M. Lyszczarz M. B. Stern	
In-Situ Monitoring of GaSb, GaInAsSb and AlGaAsSb	C. J. Vineis C. A. Wang K. F. Jensen*	9th International Conference on Metal Organic Vapor Phase Epitaxy, La Jolla, California, 30 May–4 June 1998
Recent Progress in GaInAsSb Thermophotovoltaics Grown by Organometallic Vapor-Phase Epitaxy	C. A. Wang D. C. Oakley H. K. Choi G. W. Charache*	
OMVPE Growth and Characterization of GaInAsSb for Thermophotovoltaics	C. A. Wang	16th Conference on Crystal Growth and Epitaxy, Fallen Leaf Lake, California, 7-10 June 1998

*Author not at Lincoln Laboratory.

A GaN-Based Avalanche Photodiode	S. Verghese K. A. McIntosh R. J. Molnar C. L. Chen K. M. Molvar R. L. Aggarwal I. Melngailis	56th Annual Device Research Conference, Charlottesville, Virginia, 22-24 June 1998
Flux, Penetration, Pinning and Nonlinearities	D. E. Oates	High Temperature Superconductors in High Frequency Fields, Stockholm, Sweden, 22-25 June 1998
Bromine Ion-Beam-Assisted Etching of III-V Semiconductors	W. D. Goodhue D. E. Mull S. S. Choi Y. Royter C. G. Fonstad*	40th Electronic Materials Conference, Charlottesville, Virginia, 24-26 June 1998
Preparation and Characterization of New and Novel Pb Chalcogenide-Based MBE-Grown Superlattice Structures with Enhanced Thermoelectric Figures of Merit	T. C. Harman D. L. Spears M. P. Walsh	
Optical Lithography Below 100 nm	R. R. Kunz	Microfabrication, Nanostructured Materials and Biotechnology Conference, Tegernsee, Germany, 28 June–3 July 1998
MIT Lincoln Laboratory's 0.25 μm, Low Power, High Performance, Fully Depleted SOI CMOS Technology	C. L. Keast	Semicon West '98, San Francisco, California, 13 July 1998

*Author not at Lincoln Laboratory.

Testing of Optical Materials for 193-nm Lithographic Applications	V. Liberman M. Rothschild J. H. C. Sedlacek R. S. Uttaro A. Grenville A. K. Bates C. Van Peski	SPIE International Symposium on Optical Science, Engineering and Instrumentation, San Diego, California, 19-24 July 1998
Investigation of Three-Dimensional Metallodielectric Photonic Crystals Incorporating Flat Metal Elements	K. A. McIntosh S. Verghese R. G. Atkins	

SOLID STATE
DIVISION 8

1. QUANTUM ELECTRONICS

Passively *Q*-switched Nd:YAG microchip lasers have been developed that produce up to 250 μJ per pulse at 1.064 μm, with a pulse duration of 380 ps. The infrared output has been harmonically converted to 532, 355, and 266 nm with high efficiency.

2. ELECTRO-OPTICAL MATERIALS AND DEVICES

Bromine ion-beam-assisted etching has produced smooth vertical sidewalls in GaAs, GaP, InP, AlSb, and GaSb as well as in the usual alloys formed from these materials. Our etching experience and the vapor pressure data for bromine with group III and group V elements has led us to believe that all of the various technologically important III-V binaries, ternaries, and quaternaries can be etched with this technology.

The in-plane Seebeck coefficient, Hall coefficient, and electrical resistivity of PbTe/Te superlattice structures grown by molecular beam epitaxy have been measured at 300 K. The results have shown that a significant enhancement of the in-plane Seebeck coefficient, thermoelectric power factor, and figure of merit has been achieved.

High-performance InAsSb/AlAsSb double heterostructures for mid-infrared, optically pumped lasers have been grown by molecular beam epitaxy. At ~80 K, a record optical-to-optical power conversion efficiency of 9.5% has been obtained for ~1-W long-pulse, 3.85-μm emission with 1.9-μm pumping.

Novel techniques for the accurate alignment and attachment of mass-transported microlenses to the facets of diode lasers, including tapered lasers and tapered laser arrays, have been demonstrated. Techniques for the alignment of a single element tapered laser, a GaP microlens, and a single-mode optical fiber in a compact package have also been demonstrated with an optical coupling efficiency of 60% at 980 nm.

3. SUBMICROMETER TECHNOLOGY

Line-edge roughness has been investigated experimentally for silylated top-surface imaging resist. The observed roughness has been shown to be a function of the aerial image quality and thus may limit the allowable defocus margin for the process.

Microbridge materials optimized for room-temperature infrared microbolometers have been fabricated using plasma-enhanced chemical vapor deposition. The films deposited from tetramethyldisiloxane are compatible with current CMOS processing and have been shown to have adequate thermal conductivity, infrared absorption, and mechanical strength for use as microbolometer membranes.

4. HIGH SPEED ELECTRONICS

Two-port small-signal S-parameter measurements have been performed on the first source-up 6H-SiC and drain-up 4H-SiC vertical field-effect transistors (VFETs). The 12-GHz unity current gain frequency and 4-GHz maximum frequency of oscillation obtained for the 4H-SiC VFET are the highest values obtained for any vertical transistor fabricated in SiC to date, demonstrating the potential of this technology for this material system.

5. MICROELECTRONICS

Resistive-gate charge-coupled device (CCD) technology is being reexamined as a high-yield process for some large-area CCD applications. Preliminary results on two candidate films, lightly doped polysilicon and cermet, have shown promise in meeting the requirements for the resistive gates.

6. ANALOG DEVICE TECHNOLOGY

A 1.1% bandwidth three-pole transmit filter based on stripline-like circular resonators, made using thin film superconductors, has been built and tested. The filter frequency response is independent of power up to at least 72 W, the maximum power available to us, and the intermodulation products for two 20-W input tones in-band is at least 104 dBc.

7. ADVANCED SILICON TECHNOLOGY

A study has been undertaken to assess possible hardware implementations of a new signal compression algorithm, targeted at the compression of data from infrared atmospheric sensors aboard a NASA earth observation satellite. One of the options, which offers potential advantages over the alternatives, is an application-specific integrated circuit that could be built in Lincoln Laboratory's fully depleted 0.25-μm silicon-on-insulator CMOS process.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)

2. REPORT DATE
15 August 1998

3. REPORT TYPE AND DATES COVERED
Quarterly Technical Summary: 1 May – 31 July 1998

4. TITLE AND SUBTITLE

Advanced Electronics Technology

5. FUNDING NUMBERS

C — F19628-95-C-0002
PR — 221, 222

6. AUTHOR(S)

Charles W. Niessen and David C. Shaver

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lincoln Laboratory, MIT
244 Wood St.
Lexington, MA 02420-9108

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

HQ AF Materiel Command
Wright Patterson AFB, OH 45433-5066

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

ESC-TR-97-143

11. SUPPLEMENTARY NOTES

None

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This Quarterly Technical Summary covers the period 1 May through 31 July 1998. It consolidates the reports of Division 6 (Communications and Information Technology) and Division 8 (Solid State) on the Advanced Electronics Technology Program.

14. SUBJECT TERMS

digital computers
integrated circuits
computer systems
computer network
electro-optic devices
materials research
laser research
quantum electronics
submicrometer technology
high speed electronics
microelectronics
analog device technology

15. NUMBER OF PAGES
25

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
Same as Report